

PROJECT ARES

NEXT GENERATION CYBER
SECURITY TRAINING

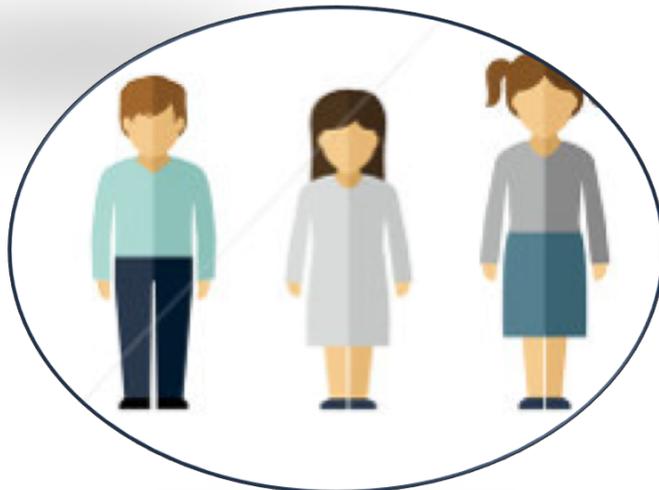
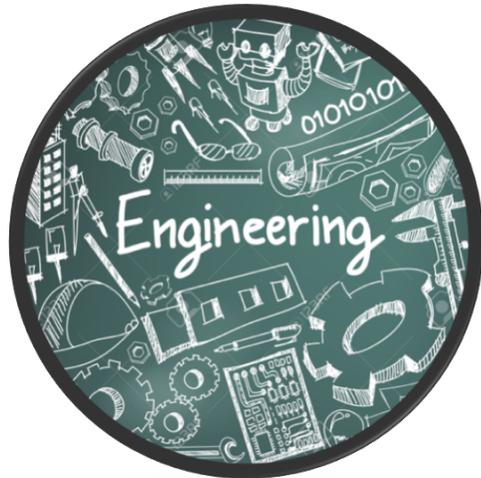
THE IMPORTANCE OF GAMIFICATION IN CYBERSECURITY TEAM TRAINING AND READINESS

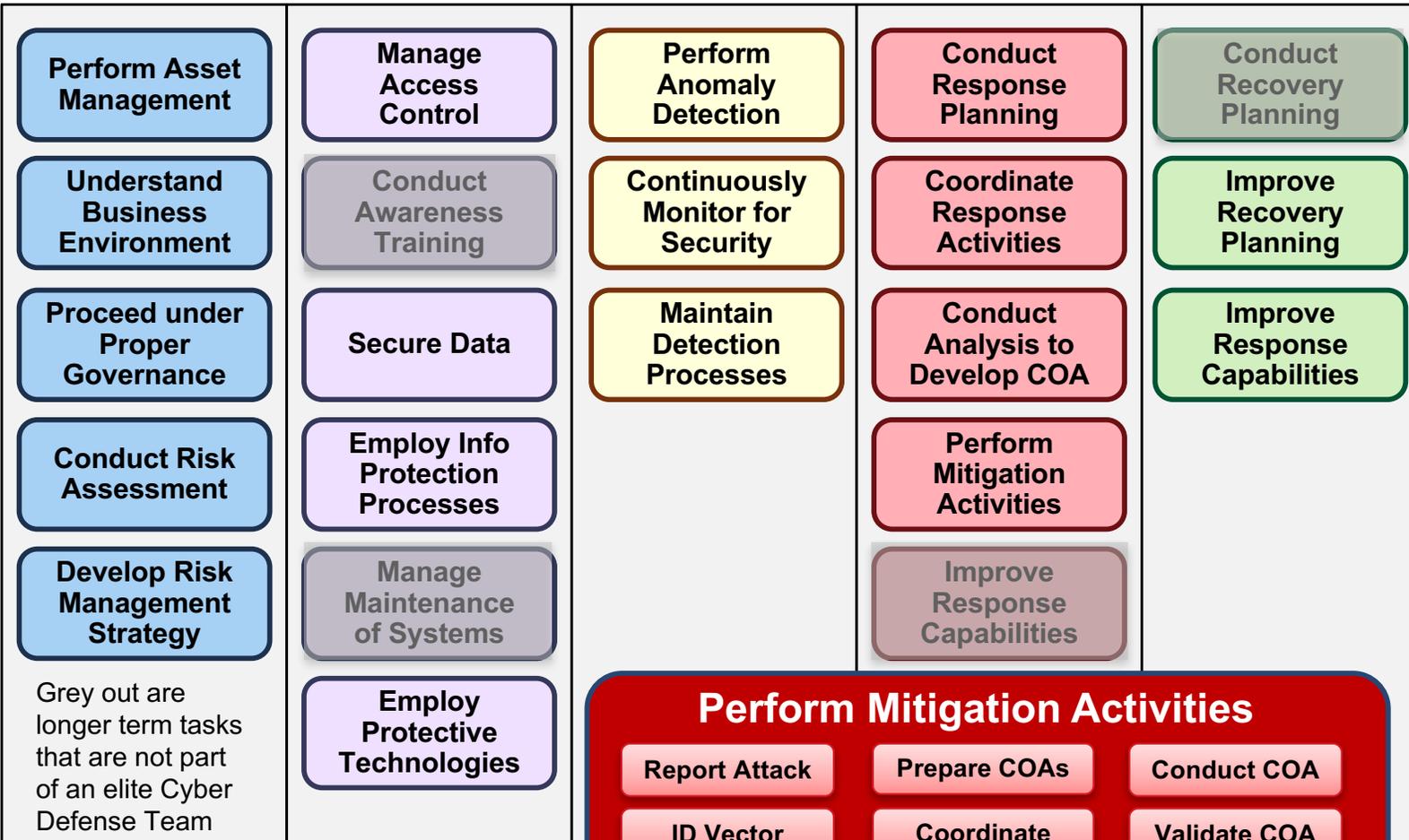
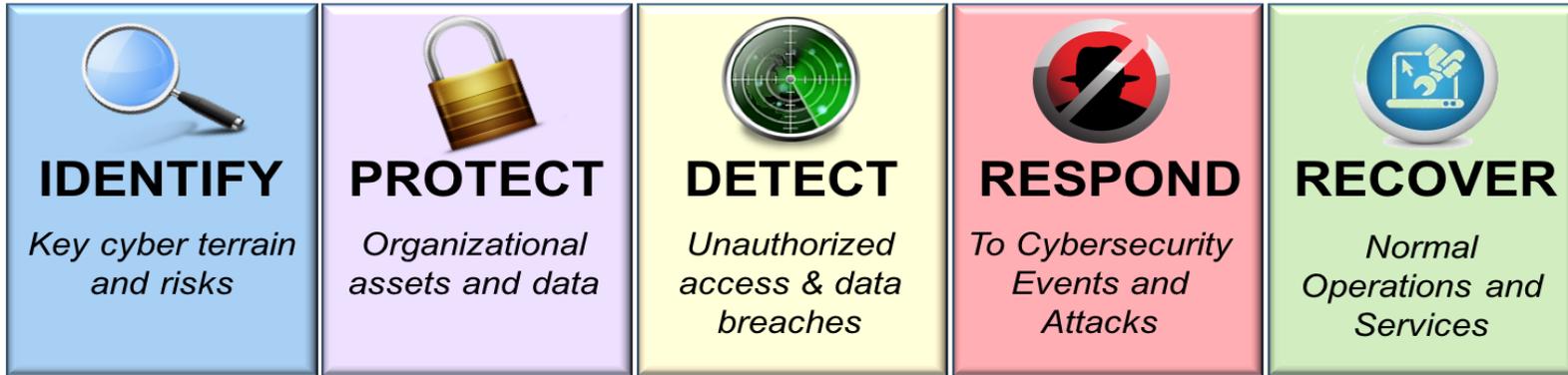
110101
0111
101



Laura Lee
Executive Vice President,
Cyber Training and Assessments
Laura.lee@circadence.com

ABOUT THE SPEAKER (

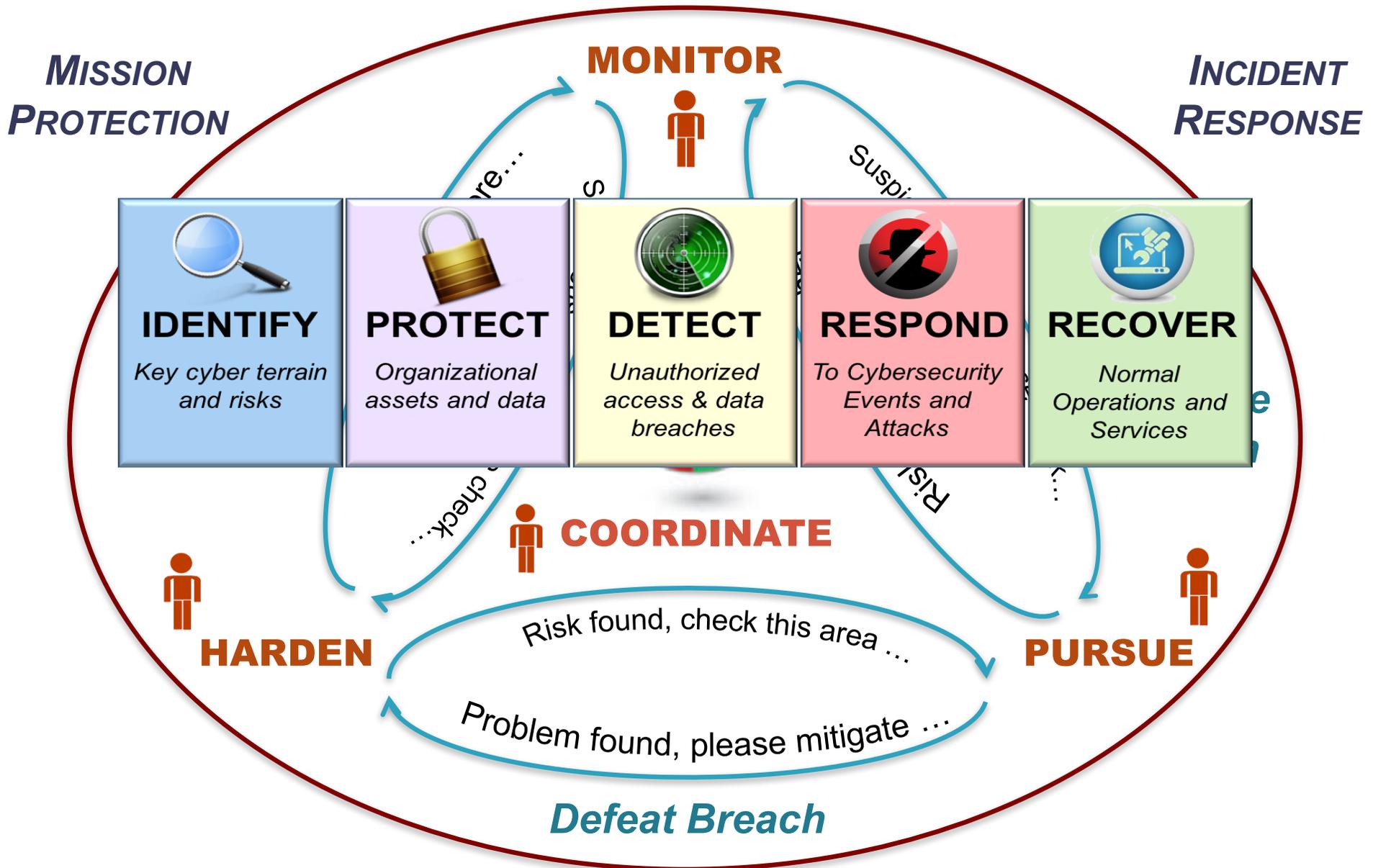




Grey out are longer term tasks that are not part of an elite Cyber Defense Team

Course of Action (COA)

CYBER DEFENSE AS A TEAM SPORT



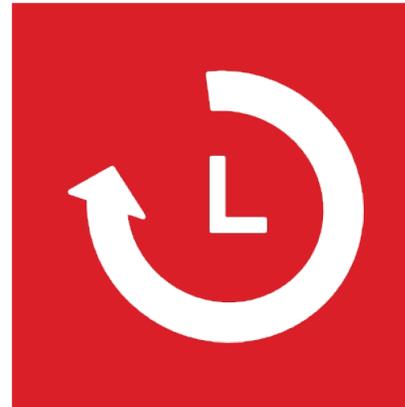
CHALLENGES FOR TRAINING CYBERSECURITY PROFESSIONALS



HIGH COSTS



SCALABILITY



AVAILABILITY



**SKILLS
RETENTION**

"As technology changes the skills needed for each profession, workers will have to adjust....[requiring] a greater emphasis on lifelong learning and on-the-job training, and wider use of online learning and video-game-style simulation."

*June 25, 2016
The Economist*

PROJECT ARES KEY TECHNOLOGIES

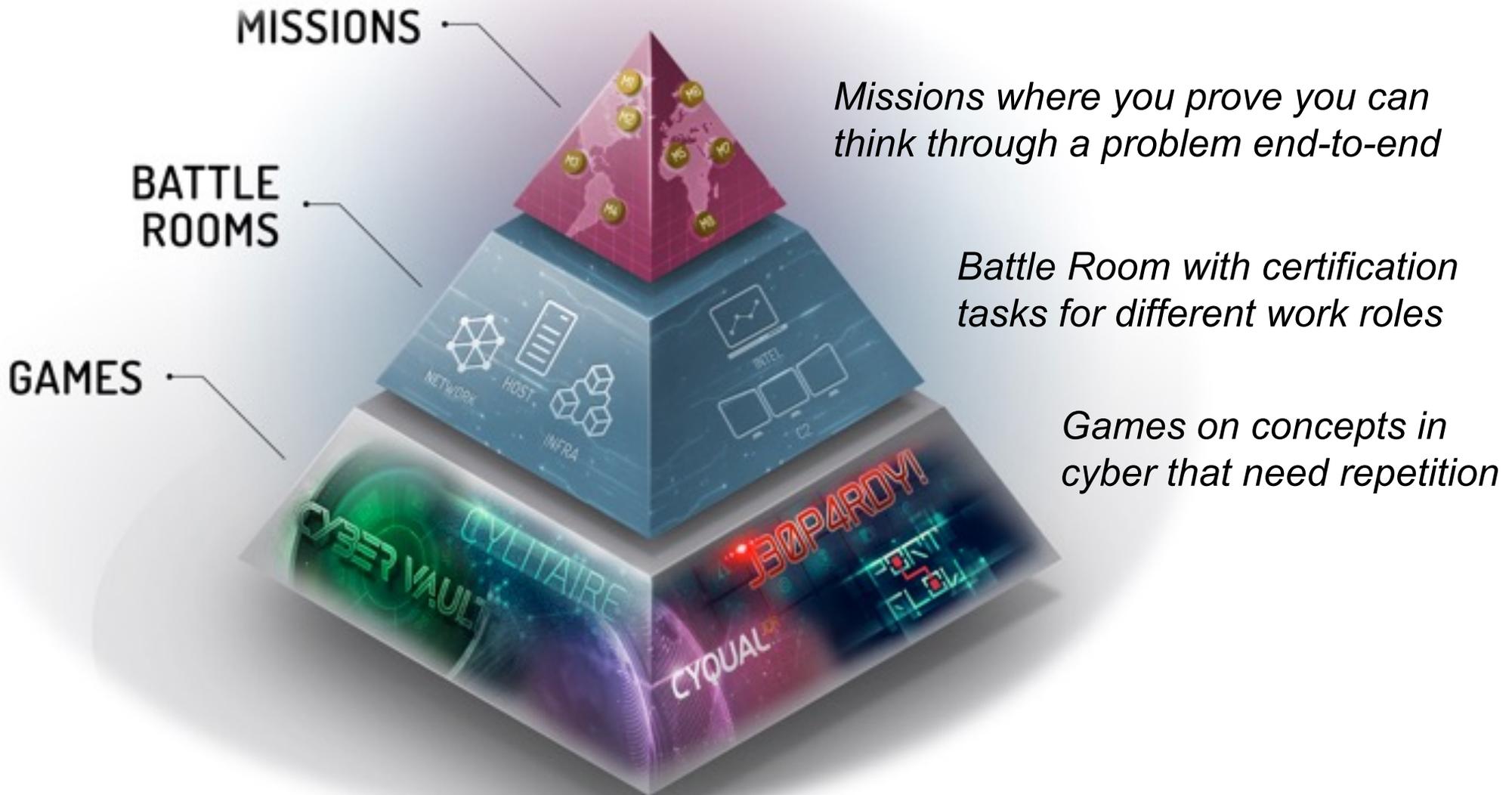
CIRCADENCE 



2016 CYBER
GOLD WINNER



TYPES OF PROJECT ARES ACTIVITIES



PROJECT ARES v3.0 (MAY 2017) (



WORLD MAP CYBER MISSIONS

Player Profile: lee, Apprentice LEVEL 1, 348 / 500 XP

Missions on Map:

- 1: Disable Botnet (Red diamond)
- 2: Stop Terrorist Financing (Red diamond)
- 3: Intercept Attack Plan (Red diamond)
- 4: Stop Malicious Processes (Blue hexagon)
- 5: Protect Financial Institution (Blue hexagon)
- 6: Respond to Phishing & Exfiltration (Blue hexagon)

Other Locations: Battle School (Yellow star), JQR Qualification (Yellow triangle)

Mission 1 Detail:
MISSION 1- DISABLE BOTNET
Infiltrate the enemy's environment and disable the command and control web server responsible for thousands of defrauded victims.
One-Sided, Offensive Mission
Small ~10, Basic Network

Chat Log (05/09/2017):

- skelly 15:24: Hopping into a defensive mission
- nmhicks 16:12: hello
- rprouty 16:24: checking for Athena

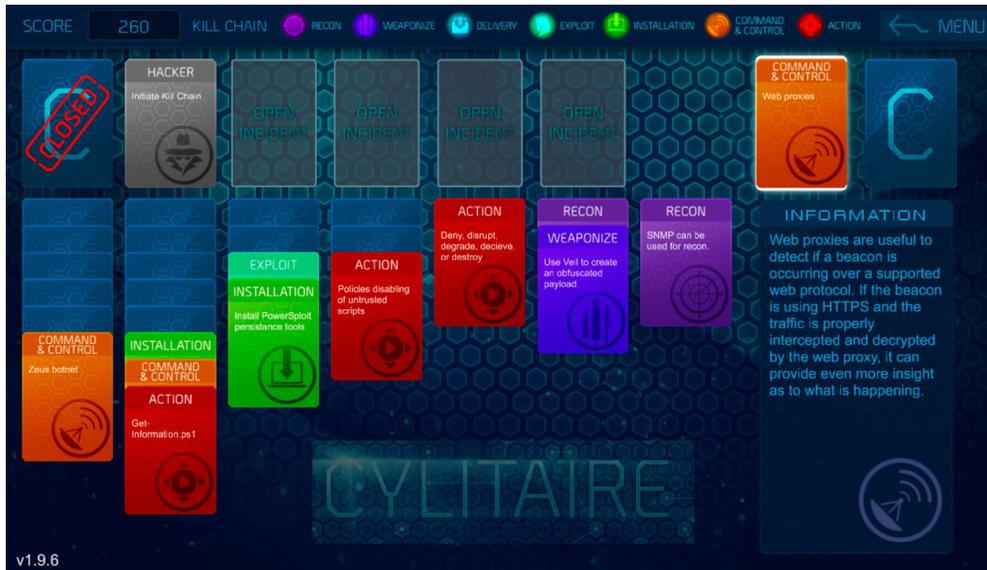
Filters: TACTICS ACTIVE, NETWORK ACTIVE, COMPLEXITY ACTIVE

Buttons: ALL PLAYERS, CHAT, PLAYERS

Footer: PROJECT ARES

PROJECT ARES CASUAL CYBER GAMES (

SCORE 260 KILL CHAIN RECON WEAPONIZE DELIVERY EXPLOIT INSTALLATION COMMAND & CONTROL ACTION MENU



HACKER
Initiate Kill Chain

EXPLOIT
Install PowerSploit persistence tools

WEAPONIZE
Use Weir to create an obfuscated payload.

INSTALLATION
Policies disabling of untrusted scripts

COMMAND & CONTROL
Web proxies are useful to detect if a beacon is occurring over a supported web protocol. If the beacon is using HTTPS and the traffic is properly intercepted and decrypted by the web proxy, it can provide even more insight as to what is happening.

RECON
SNMP can be used for recon.

ACTION
Deny, disrupt, degrade, decline, or destroy

COMMAND & CONTROL
Zeus botnet

INSTALLATION
Get: Information on ps1

COMMAND & CONTROL
Web proxies

CYLITAIRE

v1.9.6

v1.50



SCORE 160

118 119 sftp 115 443 msg-ipc https 1

SQL Services nntp ssh tcpmux 29 22

RESTART EXIT

PROJECT ARES HINT

CYBER VAULT

SCORE Score: 10

PUZZLE 2/5 ATTEMPTS REMAINING 10

146.109.25.6



CHECK

v0.7.0

MONEY \$ 200

BOOP4ROY! Kill Chain

8

In this attack technique, the attacker guesses or observes which websites the victim organization often uses and infects one or more of them with malware.

CORRECT +\$200

Click Here To Continue

What is Google Dorking?

What is a Watering Hole Attack?

What is Pass-the-Hash?

What is Phishing?

v1.6

BATTLE ROOMS FOR WORK ROLES (



BATTLE SCHOOL

BATTLE ROOM

PICK YOUR TRIAL

- Infrastructure Technician - Easy**
HISTORY
- Host Analyst - Easy**
HISTORY
- Network Analyst - Easy**
HISTORY

1-3 OF 3

Lee
Apprentice
LEVEL 1
292 / 500 XP

MISSION-1410
Team Lee

05/09/2017

athena 12:32
Welcome to your mission. I am Athena, your in-game advisor. I will join you when your mission desktop is ready.

Enter text...

PLAYERS CHAT

BATTLE SCHOOL

PROJECT ARES

BATTLE ROOM INDIVIDUAL SKILLS (

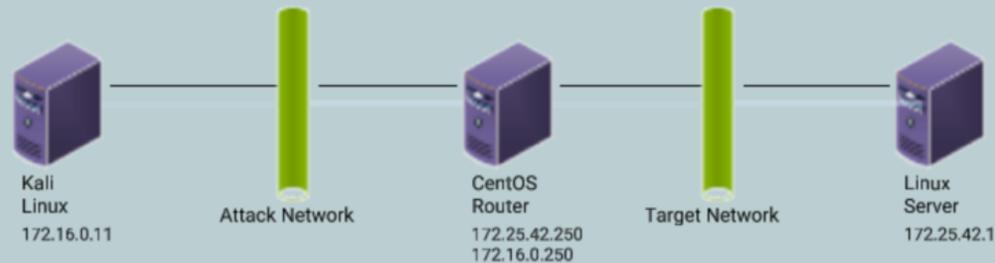
BATTLE ROOM . INFRASTRUCTURE TECHNICIAN - EASY

Time: 0:20:47 Score: 3

TASKS 2 OF 38

All Trials

- Using iptables, identify all rules that are in place on the Kali1 system (id:19)
- Use netstat to obtain a list of all active (open, established, wait) network connections without doing name lookups (id:20)
- Use nmap to perform a version scan to identify services and software running on the *target* (id:21)
- Use apt-get to install the openvas package on the Kali1 system from the configured repository (id:22)
- Use hydra to determine whether there are easily guessable passwords for the root user using the SSH service on the *target* (id:23)
- Use apt to get a list of all of the installed packages on the Kali Linux system (id:24)



Running 0:20

ilee
Apprentice
LEVEL 1
3 / 500 XP

ALL PLAYERS

01/04/2017

rob_player 10:09

hello

rob_player 21:31

how do i discover open ports on host

04/01/2017

ilee 18:52

Good evening fellow team mates

04/17/2017

rprouty 21:46

good evening

ilee 21:57

Hello Mate

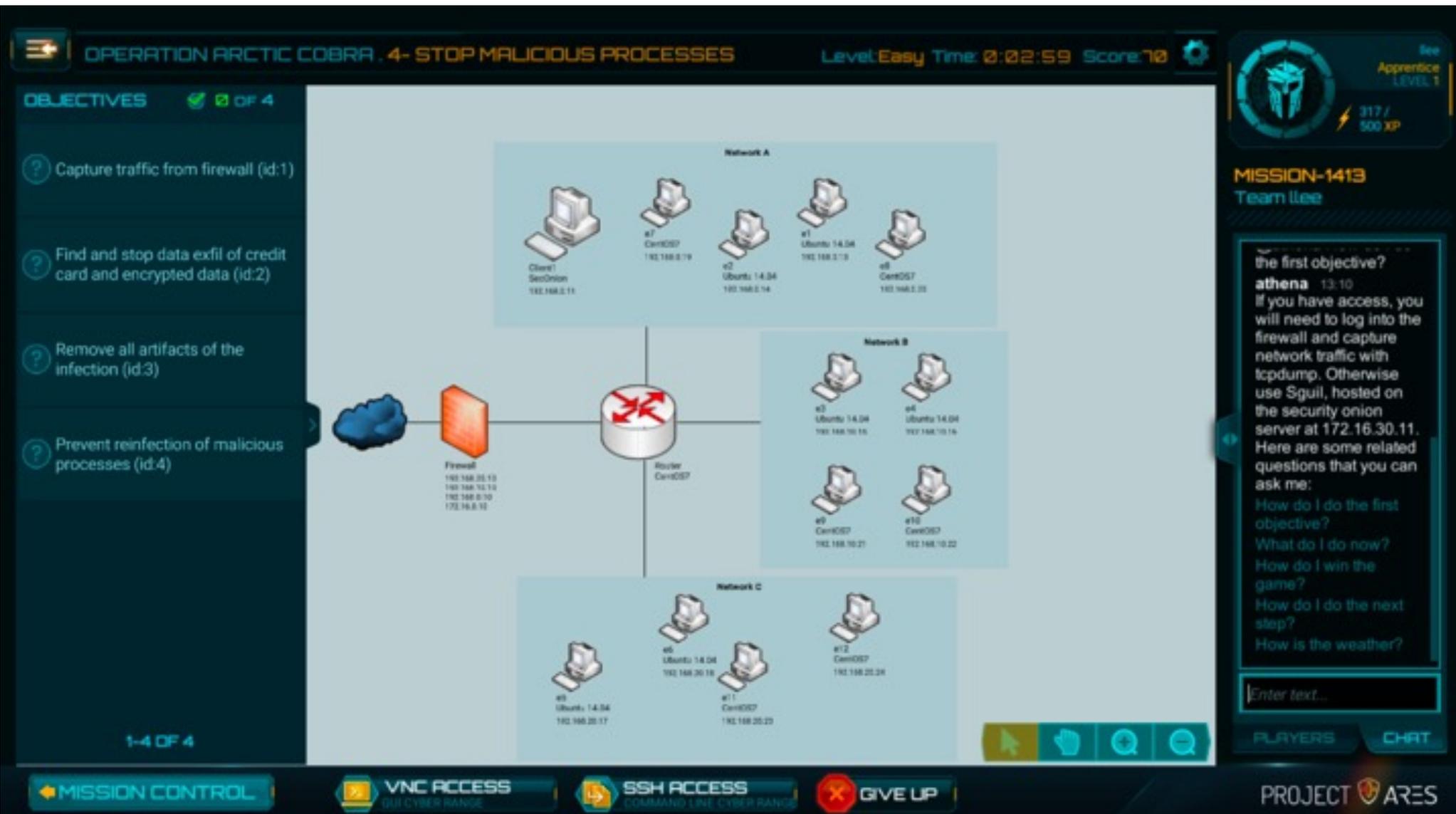
Enter text...

PLAYERS

CHAT

PROJECTARES

MISSION PLAY (INDIVIDUAL, CREW AND TEAM PLAY)



The screenshot displays the 'OPERATION ARCTIC COBRA' mission interface. At the top, it shows '4- STOP MALICIOUS PROCESSES', 'Level: Easy', 'Time: 0:02:59', and 'Score: 70'. The left sidebar lists four objectives: 1. Capture traffic from firewall (id:1), 2. Find and stop data exfil of credit card and encrypted data (id:2), 3. Remove all artifacts of the infection (id:3), and 4. Prevent reinfection of malicious processes (id:4). The main area shows a network diagram with three sub-networks (A, B, and C) connected to a central router. Network A contains a client and three servers. Network B contains four servers. Network C contains three servers. A firewall is connected to the left side of the network. The right sidebar shows the player's status as 'Apprentice LEVEL 1' with 317/500 XP, and a chat window with a list of questions related to the first objective. At the bottom, there are buttons for 'MISSION CONTROL', 'VNC ACCESS', 'SSH ACCESS', and 'GIVE UP', along with the 'PROJECT ARES' logo.

OPERATION ARCTIC COBRA . 4- STOP MALICIOUS PROCESSES Level: Easy Time: 0:02:59 Score: 70

OBJECTIVES 3 OF 4

- 1. Capture traffic from firewall (id:1)
- 2. Find and stop data exfil of credit card and encrypted data (id:2)
- 3. Remove all artifacts of the infection (id:3)
- 4. Prevent reinfection of malicious processes (id:4)

Network A

- Client SecOinion 192.168.0.11
- #7 CentOS 192.168.0.19
- #2 Ubuntu 14.04 192.168.0.14
- #1 Ubuntu 14.04 192.168.0.13
- #8 CentOS 192.168.0.20

Network B

- #3 Ubuntu 14.04 192.168.10.15
- #4 Ubuntu 14.04 192.168.10.14
- #9 CentOS 192.168.10.21
- #10 CentOS 192.168.10.22

Network C

- #6 Ubuntu 14.04 192.168.20.17
- #5 Ubuntu 14.04 192.168.20.15
- #11 CentOS 192.168.20.23
- #12 CentOS 192.168.20.24

Firewall 192.168.20.13, 192.168.10.10, 192.168.0.10, 172.16.8.10

Router CentOS

MISSION-1413
Team Lee

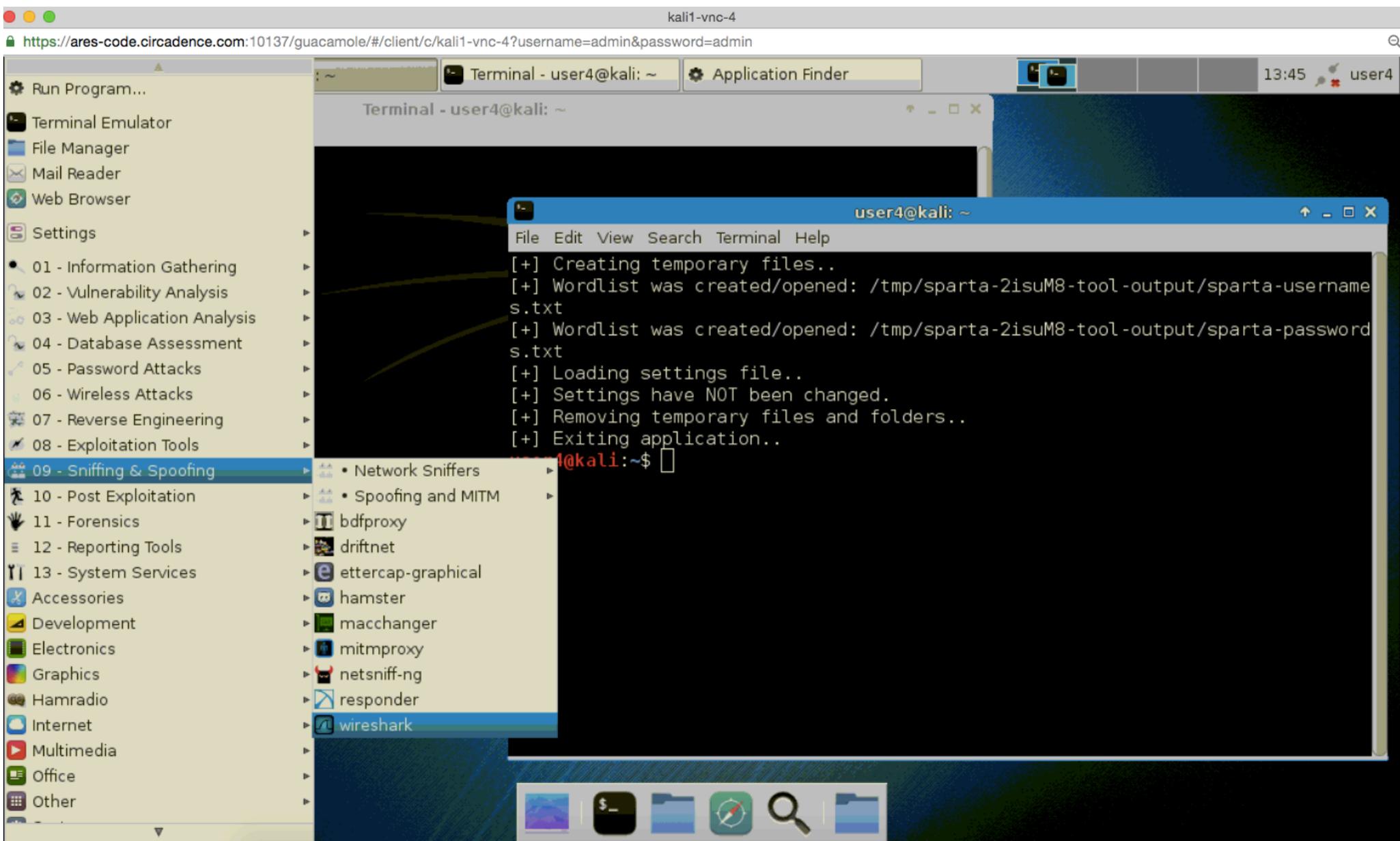
the first objective?
athena 13:10
If you have access, you will need to log into the firewall and capture network traffic with tcpdump. Otherwise use Sguil, hosted on the security onion server at 172.16.30.11. Here are some related questions that you can ask me:
How do I do the first objective?
What do I do now?
How do I win the game?
How do I do the next step?
How is the weather?

Enter text...

PLAYERS CHAT

MISSION CONTROL VNC ACCESS GUI CYBER RANGE SSH ACCESS COMMAND LINE CYBER RANGE GIVE UP PROJECT ARES

CYBER TOOLS AVAILABLE ON MISSION (



The screenshot displays a Kali Linux desktop environment accessed via a VNC client. The browser address bar shows the URL: <https://ares-code.circadence.com:10137/guacamole/#/client/c/kali1-vnc-4?username=admin&password=admin>. The desktop features a terminal window titled "Terminal - user4@kali: ~" and an application finder window. A menu is open, showing various categories of tools. The "09 - Sniffing & Spoofing" category is expanded, listing several tools including Wireshark, which is highlighted. The terminal window shows the output of a program execution, including messages about creating temporary files, wordlists, and loading settings.

Terminal Output:

```
user4@kali: ~  
File Edit View Search Terminal Help  
[+] Creating temporary files..  
[+] Wordlist was created/opened: /tmp/sparta-2isuM8-tool-output/sparta-username  
s.txt  
[+] Wordlist was created/opened: /tmp/sparta-2isuM8-tool-output/sparta-password  
s.txt  
[+] Loading settings file..  
[+] Settings have NOT been changed.  
[+] Removing temporary files and folders..  
[+] Exiting application..  
user4@kali:~$
```

MISSION ASSESSMENT

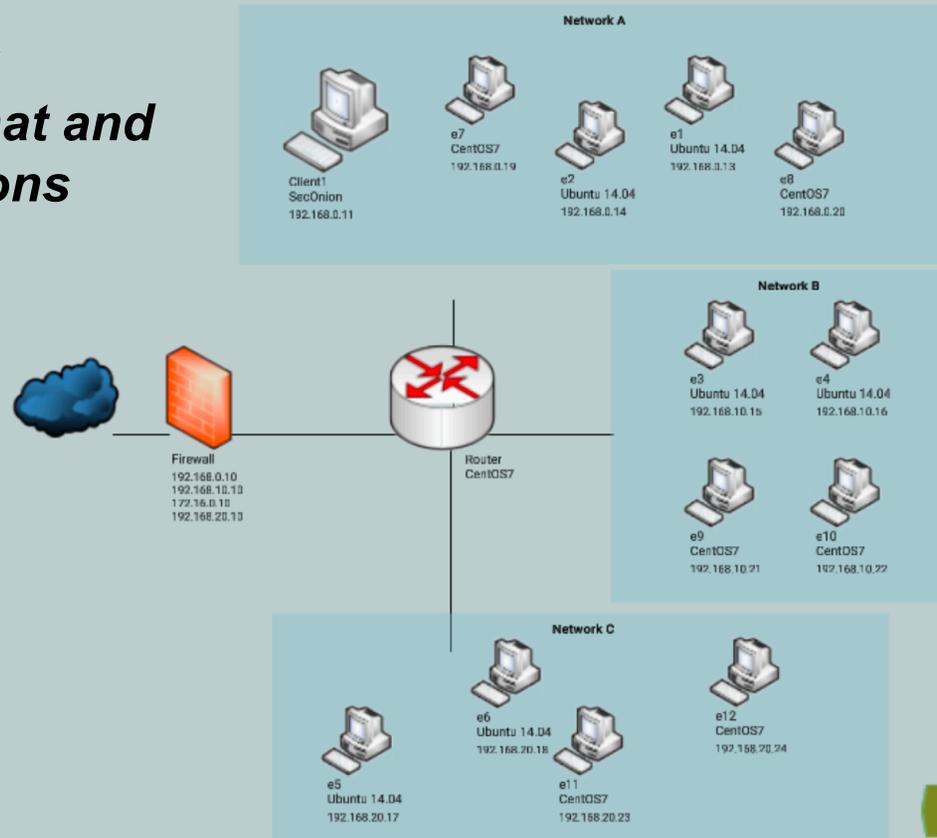
ASSESSMENT . 4- STOP MALICIOUS PROCESSES

Level: Easy Score: Time: 0:58:00

STATE: PAUSED 0.0.47bc6

Team llee
2017-01-20T01:03:20Z
Session Id: 1775

Replay of user commands, chat and opponent actions



Mission Objectives

- ✓ Capture traffic from firewall
- ✓ Find and stop data exfil. of credit card and encrypted data
- Remove all artifacts of first infection
- Prevent reinfection of malicious process

```
[18] llee: ssh 192.168.0.10
[22] llee: wireshark out.pcap
[23] llee: /usr/bin/dumpcap -D -Z none
[24] llee: /usr/bin/dumpcap -D -Z none
[36] llee: ssh testuser@192.168.20.23
[66] llee: ls --color=auto
[67] llee: ssh testuser@192.168.20.23
```

0:39:27  0:58:00

Events Chats

MISSION SCORE

WORLD MAP . MISSION SELECT



 APPRENTICE L4
1,034,233 / 2,000,000 XP
  

COMPLETE MISSION I - DISABLE BOTNET DURATION - 03:30



203

Quiz



122

Recon Network



442

Objectives



767

Total Points

 23 XP

 22 XP

 12 XP

 57 XP

 1,034,233 XP

LEVEL UP 2,000,000

LEADERBOARD

	Team Name	Duration	Score
1	 Team Hernandez	03:12:54	234,032
2	 Team Tucker	01:21:33	212,840
3	 Team Farmer	03:43:54	204,304
4	 Team Price	04:22:24	203,597
5	 Team Reid	01:14:55	203,232
15	 Team Carson	02:33:21	150,207

MISSION COMPLETE: TROPHY CENTER

0.0.47bc6

WORLD MAP. BATTLE SCHOOL



llee

global-chat

TROPHY CENTER

DIFFICULTY LEVELS COMPLETED

Current awards and past mission history is available to replay



Operation Goatherd
1- Disable Botnet

Highest Level Achieved



 HISTORY



Operation Arctic Cobra
4- Stop Malicious Processes

Highest Level Achieved



 HISTORY



Operation Bear Treat
2- Stop Terrorist Financing

No History Available



Operation Wounded Bear
5- Protect Financial Institution

Highest Level Achieved



 HISTORY



Operation Desert Whale
3- Intercept Attack Plans

No History Available



Operation Angry Tiger
6- Respond to Phishing & Exfiltration

No History Available

you do that or want to play.

01/16/2017

skelly 12:27
@llee looks like I was ghosting

01/19/2017

nmhicks 10:41
hello!
nmhicks 11:20
@llee I'm connected from their workspaces
nmhicks 11:31
@llee all tests complete - VNC and SSH both work from the team workspaces

Enter text...

Players

Chat

INVITE PLAYERS

 MENU

PROJECT  ARES

BADGES AND SKILLS

Players earn experience points as they play games, work in Battle Room or go on mission

WORLD MAP . MISSION SELECT

ALL | IN PROGRESS | COMPLETED | FUTURE

 APPRENTICE L4
1,034,233 / 2,000,000 XP
 more



DIGITAL FORENSICS



COMPUTER LANGUAGES



NETWORK DEFENSE



COMPUTERS & ELECTRONICS



CRIMINAL LAW



CRYPTOGRAPHY



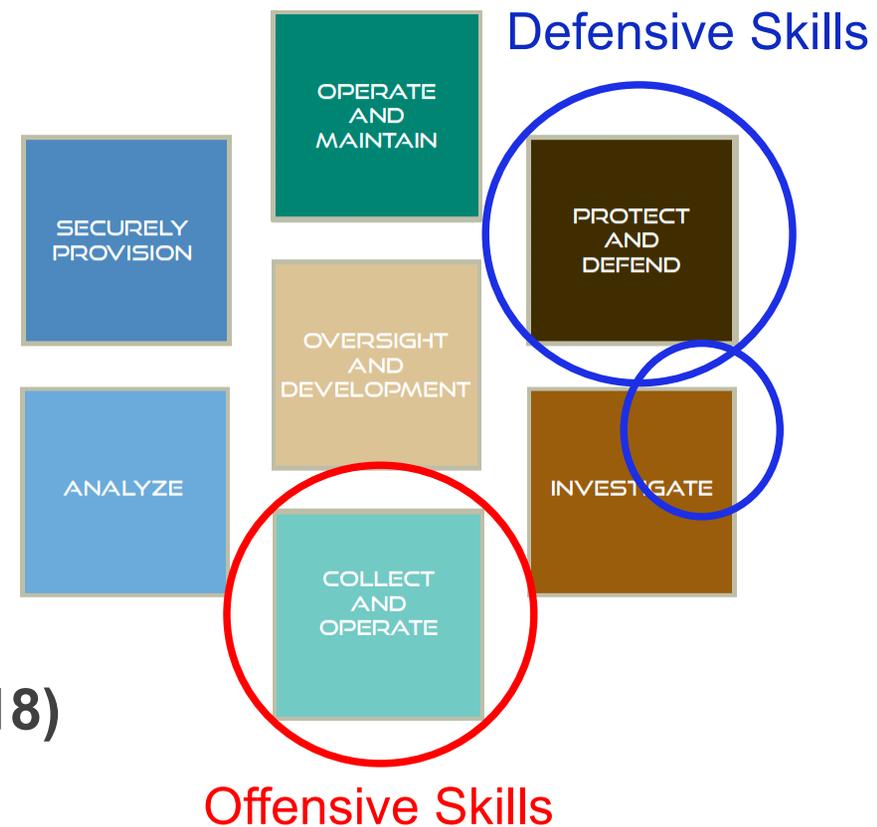
ENTERPRISE ARCHITECTURE



IDENTITY MANAGEMENT



- **Categories – Protect & Defend, Investigate (Digital Forensics)**
- **Specialty Areas (4)**
 - Enterprise Network Defense Analysis
 - Incident Response
 - Infrastructure support
 - Vulnerability Assessment and Mgmt
- **Work Roles (45)**
 - Security Analyst
 - Incident Analyst
 - Penetration Tester....
- **Competencies (~200 combined into 18)**
- **Tasks (~115)**



EVERYTHING I LEARNED, I LEARNED FROM ENDER'S GAME



"I need you to think of solutions to problems we haven't seen yet. I want you to try things that no one has ever tried because they're absolutely stupid."
-- Ender Wiggins

The games are designed to harness the creativity of children and channel that to mold them into skilled soldiers, tacticians, and leaders to save the world.

Ender's Game is a 1985 military science fiction novel by American author Orson Scott Card and 2013 LionsGate Film.



CIRCADENCE 

www.circadence.com %